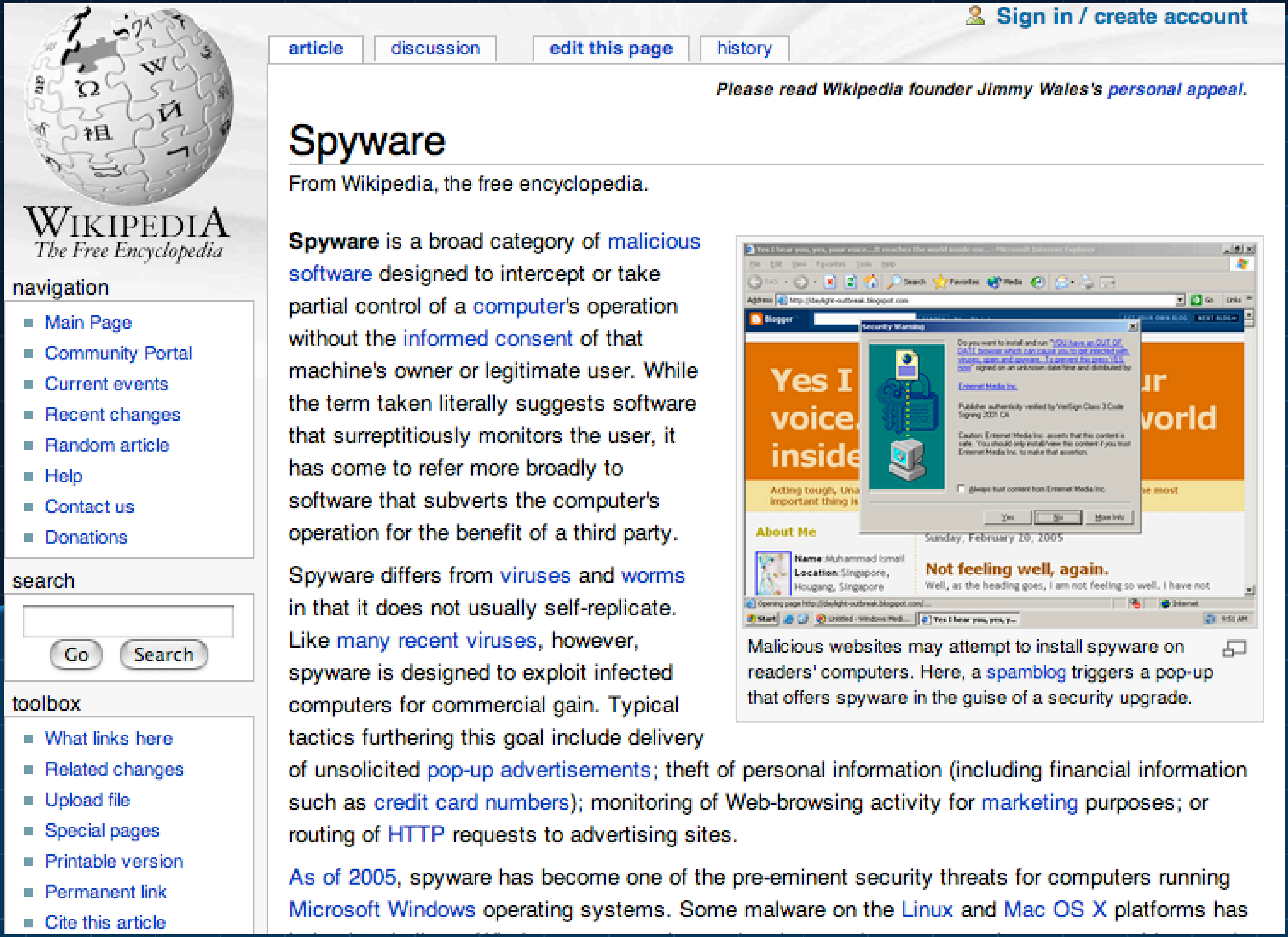
Spyware

What it is and what to do about it.

What is Spyware?

- Spyware
- Adware
- Tracking



Please read Wikipedia founder Jimmy Wales's personal appeal.

Spyware

From Wikipedia, the free encyclopedia.

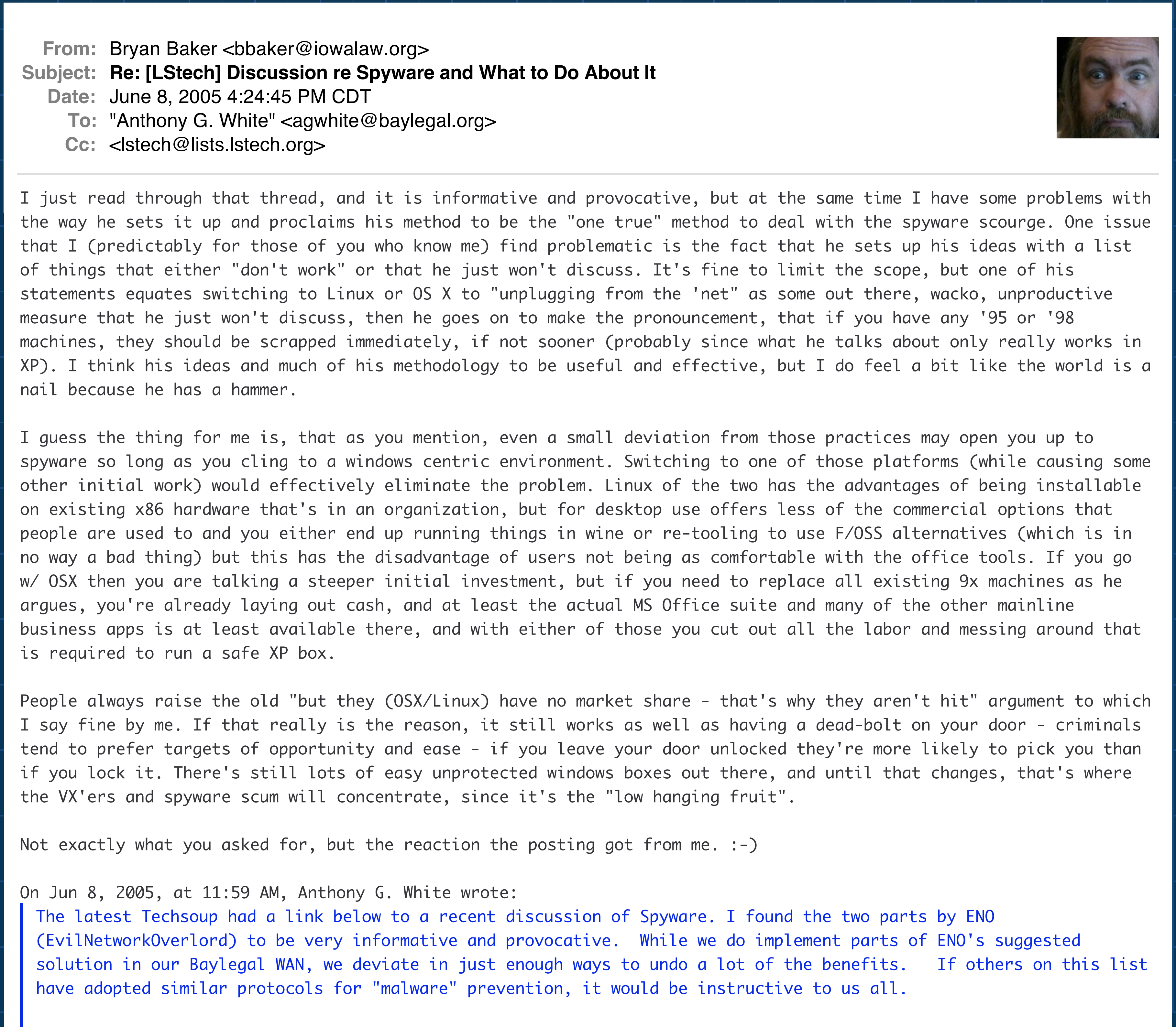
Spyware is a broad category of malicious software designed to intercept or take partial control of a computer's operation without the informed consent of that machine's owner or legitimate user. While the term taken literally suggests software that surreptitiously monitors the user, it has come to refer more broadly to software that subverts the computer's operation for the benefit of a third party.

Malicious websites may attempt to install spyware on readers' computers. Here, a spamblog triggers a pop-up that offers spyware in the guise of a security upgrade.

Spyware differs from viruses and worms in that it does not usually self-replicate. Like many recent viruses, however, spyware is designed to exploit infected computers for commercial gain. Typical tactics furthering this goal include delivery of unsolicited pop-up advertisements; theft of personal information (including financial information such as credit card numbers); monitoring of Web-browsing activity for marketing purposes; or routing of HTTP requests to advertising sites.

As of 2005, spyware has become one of the pre-eminent security threats for computers running Microsoft Windows operating systems. Some malware on the Linux and Mac OS X platforms has

Why am I here?



From: Bryan Baker <bbaker@iowalaw.org>
Subject: **Re: [LStech] Discussion re Spyware and What to Do About It**
Date: June 8, 2005 4:24:45 PM CDT
To: "Anthony G. White" <agwhite@baylegal.org>
Cc: <lstech@lists.lstech.org>

I just read through that thread, and it is informative and provocative, but at the same time I have some problems with the way he sets it up and proclaims his method to be the "one true" method to deal with the spyware scourge. One issue that I (predictably for those of you who know me) find problematic is the fact that he sets up his ideas with a list of things that either "don't work" or that he just won't discuss. It's fine to limit the scope, but one of his statements equates switching to Linux or OS X to "unplugging from the 'net" as some out there, wacko, unproductive measure that he just won't discuss, then he goes on to make the pronouncement, that if you have any '95 or '98 machines, they should be scrapped immediately, if not sooner (probably since what he talks about only really works in XP). I think his ideas and much of his methodology to be useful and effective, but I do feel a bit like the world is a nail because he has a hammer.

I guess the thing for me is, that as you mention, even a small deviation from those practices may open you up to spyware so long as you cling to a windows centric environment. Switching to one of those platforms (while causing some other initial work) would effectively eliminate the problem. Linux of the two has the advantages of being installable on existing x86 hardware that's in an organization, but for desktop use offers less of the commercial options that people are used to and you either end up running things in wine or re-tooling to use F/OSS alternatives (which is in no way a bad thing) but this has the disadvantage of users not being as comfortable with the office tools. If you go w/ OSX then you are talking a steeper initial investment, but if you need to replace all existing 9x machines as he argues, you're already laying out cash, and at least the actual MS Office suite and many of the other mainline business apps is at least available there, and with either of those you cut out all the labor and messing around that is required to run a safe XP box.

People always raise the old "but they (OSX/Linux) have no market share - that's why they aren't hit" argument to which I say fine by me. If that really is the reason, it still works as well as having a dead-bolt on your door - criminals tend to prefer targets of opportunity and ease - if you leave your door unlocked they're more likely to pick you than if you lock it. There's still lots of easy unprotected windows boxes out there, and until that changes, that's where the VX'ers and spyware scum will concentrate, since it's the "low hanging fruit".

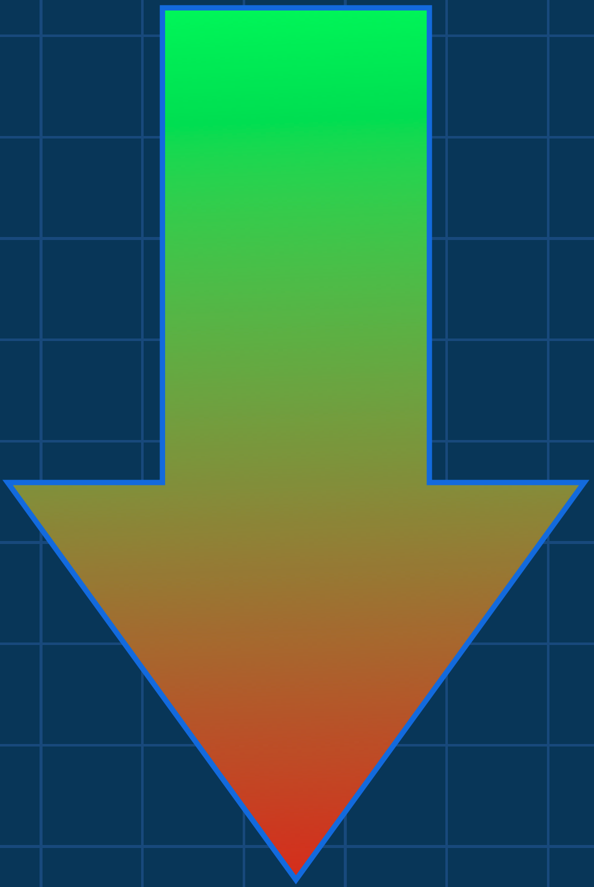
Not exactly what you asked for, but the reaction the posting got from me. :-)

On Jun 8, 2005, at 11:59 AM, Anthony G. White wrote:

> The latest Techsoup had a link below to a recent discussion of Spyware. I found the two parts by ENO (EvilNetworkOverlord) to be very informative and provocative. While we do implement parts of ENO's suggested solution in our Baylegal WAN, we deviate in just enough ways to undo a lot of the benefits. If others on this list have adopted similar protocols for "malware" prevention, it would be instructive to us all.

What can we do?

- Education
- Prevention
- Migration
- Mitigation



Education

- Self
  - Keep yourself informed
  - Lead by Example
- Management
  - Buy In
  - Support
- Users

Prevention
(Windows™ & Internet Explorer)

- Standardize on Windows XP™ at a minimum.
- Don’t give administrative privileges to normal user accounts.
- Use a content filtering proxy server.
- Use desktop software to monitor for registry and configuration changes.
- Keep up to date on patches and service packs

Migration

- Hand in hand with prevention
- Application migration
  - Web Browser
  - Email
- Platform migration
  - Linux
  - Mac OS X

Mitigation

- Tools such as AdAware and Spybot can automate some of the removal
- You can never be sure you got everything
- Complete removal may be impossible
- Reinstallation or reimaging is often faster and more consistent

There is hope

- With proper education, prevention, and some migration, problems can be greatly reduced or eliminated
- User education makes the greatest impact

Open Discussion